The National Science Foundation
Office of Polar Programs
United States Antarctic Program

Information Resource Management Directive 5000.6
Acceptable Use of USAP Information Resources

Organizational Function	Information Resource Management	Policy Number	5000.6
		Issue Date	1 August 2004
Policy Category	Information Security Policies and Procedures	Effective Date	1 August 2004
		Review On	1 August 2006
Subject	Acceptable Use of Resources	Authorized By	Director, OPP
Office of Primary Responsibility	National Science Foundation Office of Polar Programs Polar Research Support Section	Responsible Official	Mr. Patrick D. Smith Technology Development Manager
Address	Suite 755 4201 Wilson Blvd Arlington, VA 22230	Phone	703.292.8032
		Fax	703.292.9080
		Web	www.nsf.gov/od/opp
Distribution	USAP-Wide	Status	Final Policy
Online Publication	www.polar.org/infosec/index.htm		

1. PURPOSE

This directive establishes the acceptable use policy for U.S government information systems supporting the National Science Foundation (NSF) Office of Polar Programs (OPP), United States Antarctic Program (USAP). This includes the use of information systems and resources, computers, telephones, Internet access, electronic mail (email), voice mail, reproduction equipment, facsimile systems, and other forms of electronic communications.

2. BACKGROUND

U.S. Antarctic Program information resources provide critical support to USAP mission areas, such as life safety, station and vessel operations, science activities, and personnel morale and general welfare. Using information resources for inappropriate, unauthorized, or unlawful activities can seriously undermine the program's ability to accomplish its mission and in some cases could result in serious injury or even death. USAP participants shall make every effort to employ USAP information resources in an appropriate and acceptable manner, according to the guidelines in this and other policies

3. GUIDING PRINCIPLES

In establishing practices for acceptable use, the program will follow these guiding principles:

- USAP information resources, especially at the Antarctic research stations and aboard the research vessels, may be used for certain personal uses, in a manner that does not interfere with the program's mission. All mission activities take precedence over personal activities at all times.
- Systems and network administrators, and others who may be exposed to a participant's personal communications as a part of their normal duties, are in a position of trust and will be held accountable for violations of that trust on their part.
- The National Science Foundation is not a common carrier, and does not possess the requisite infrastructure and resources necessary to guarantee the privacy of information processed or stored on USAP information systems or networks. Users of USAP systems agree that the government and its representatives are not responsible for the loss of personal information, or for the disclosure of personal information as a result of unauthorized activity by participants or by others outside the program.
- Participants and their leaders are expected to use good judgment in appropriate use of program assets consistent with the purposes of this policy. However, the final determination regarding what constitutes appropriate use consistent with this policy is reserved to NSF management in coordination with the participant's organization.

4. POLICY

The National Science Foundation provides information systems for the purpose of transacting official business of the U.S. Antarctic Program. The NSF establishes Rules of Behavior for the proper use of these systems. Any non-program use of USAP information resources must be authorized by management or this policy.

4.1. Official Business

Official business broadly includes any information processing that is required as part of an individual's work responsibilities. Official business includes, but is not limited to, the performance of USAP work-related duties in position descriptions, professional training and class work, work covered under grant agreements with the NSF, tasks directed via NSF contracts, agreements with international partners, and support activities related to NSF contract tasking.

4.2 Personal Use

Personal use broadly includes any information processing that is conducted in support of activities that do not constitute official business. A personal use activity is typically one in which the individual user, or a non-USAP entity is the primary beneficiary. Participants who use program assets for personal purposes are responsible for any and all

liability that may arise from such personal use to include any violation of law, regulation or policy during such use.

4.3 Rules of Behavior

The Office of Polar Programs will create and maintain Rules of Behavior that explain the acceptable and prohibited uses of all USAP information resources.

4.3.1 Enterprise Rules of Behavior

The Enterprise Rules of Behavior apply to all users of the USAP information infrastructure. Each year, the Information Security Manager will compile the Enterprise Rules of Behavior, and publish them to coincide with the start of the science planning process. The Enterprise Rules of Behavior must be presented to each user of the USAP information infrastructure. All users must acknowledge, in writing or other verifiable means, that they have received the Rules of Behavior, and consent to follow the Rules.

4.3.2 Site Rules of Behavior

Each USAP operating location, following review and approval by OPP, may prepare supplemental Rules of Behavior for users at that location,. The supplemental Rules of Behavior may not be less stringent than the Enterprise Rules of Behavior, unless approved by OPP. Site Rules of Behavior must be published by 30 September of each year to coincide with the start of the austral summer season. The Site Rules of Behavior must be presented to each user of the site's information infrastructure. All users must acknowledge, in writing or other verifiable means, that they have received the Rules of Behavior, and consent to follow the Rules.

4.3.3 System Rules of Behavior

Each USAP information system owner will establish Rules of Behavior for that system, which will generally supplement the Enterprise Rules of Behavior. The System Rules of Behavior may not be less stringent than the Enterprise Rules of Behavior, unless approved by OPP. The System Rules of Behavior must be presented to each user of the USAP information system. All users must acknowledge, in writing or other verifiable means, that they have received the Rules of Behavior, and consent to follow the Rules.

4.3 Rules of Behavior Organization

The Rules of Behavior will be organized to clearly explain the roles and responsibilities of system users, systems administrators, and others needing access to the infrastructure or system.

4.4 Rules of Behavior Content

The Enterprise Rules of Behavior must address, at minimum, the Acceptable and Prohibited Uses of the USAP information infrastructure as related to the following issues:

- No expectation of Privacy while using government resources
- Ownership of Information

- Use of Antivirus Applications
- Copyright and Intellectual Property Issues
- Dual-Use Status
- Personal use of Telephone, Facsimile, Electronic Mail Internet Use
- Encryption of Personal Communications
- Third Party Software, Freeware and Shareware
- Mailing Lists
- Personal Business or Commercial Uses
- Illegal Activities
- Adverse Activities
- No processing of classified information
- Hostile Environment
- Prohibited Email Activities
- Personal Information Services
- Chat Room and News Group Participation
- Political Activities
- Gaming
- Prohibited Business and Commercial uses
- Prohibited Network Activities
- Use of information protocols determined to be detrimental to the infrastructure

5. APPLICABILITY AND COMPLIANCE

This policy applies to all information resources, systems, and technology and to all users of these resources, systems and technology within the USAP operating environment or connected to the USAP information infrastructure. Compliance with this policy and the Rules of Behavior is as indicated in USAP Information Security Policy 5000.1, *The USAP Information Security Program*. In addition to the stipulations in 5000.1, failure to comply with this policy or with the

6. RESPONSIBILITIES

Within the NSF and the USAP, several elements have specific responsibilities directly related to the acceptable use of USAP information resources.

6.1 NSF Head of Polar Research Support Section

The Head of the Polar Research Support Section adjudicates disputes over the interpretation of the Rules of Behavior and serves as approval authority for requests to waive the Rules.

6.2 USAP Information Security Manager

The USAP Information Security Manager (ISM) develops and implements the Enterprise Rules of Behavior for the USAP information infrastructure, and oversees the development and implementation of site and system rules of behavior as required.

6.3 USAP Station Managers

The USAP Station Managers ensure the Rules of Behavior are implemented at their station, and develop site rules of behavior as required.

6.4 USAP Information Systems Managers

The USAP Information Systems Managers ensure the Rules of Behavior are implemented within their systems, and develop system rules of behavior as required.

6.5 USAP Information Systems Users

All USAP Information Systems Users ensure they comply with the Rules of Behavior.

7. POLICY IMPLEMENTATION

7.1 Implementation

The USAP Information Security Manager will review and update the Enterprise Rules of Behavior each year, using the policy development process referenced in USAP Information Security Policy 5000.2, *Information Security Organization and Administration*. USAP site management and system owners will create and implement Rules of Behavior for systems under their control, as required, after review and approval by NSF OPP.

7.2 Requests for Waivers to the Rules of Behavior

Requests to waive the Rules of Behavior shall be submitted in writing to the Head of Polar Research Support, Office of Polar Programs. To ensure proper and adequate consideration of the waiver, requests must be submitted independent of any other documents submitted to OPP or the NSF, and may not be included in proposal documents such as the Operations Readiness Worksheet (ORW) or the Science Information Package (SIP).

7.3 Policy Review

The USAP Information Security Program Manager will review this policy in conjunction with major changes to the information infrastructure, as part of the USAP's participation in agency security audits, after each breach in system security, or every two years. The ISM will submit policy changes and new policies for review and approval by NSF OPP

8. AUTHORITY

Publication of this policy is in conformance with the authority of the National Science Foundation Act of 1950, as amended and extended, the Federal Information Security Management Act of 2002 and NSF Manual 7, The NSF Information Security Handbook.

KARL A. ERB

Director